IETF 97

Bundled Domain Names

John Levine / j@jl.ly

The Problem(s)

- Domain names map poorly onto human names and terms
- We want several names to work “the same”
- We don’t understand how to do that
- We don’t understand what “the same” means

In and out of scope

IN

- Handle modest groups of names
- Automate bundle management

OUT

- Huge groups of names
  - M^N: M variants per character, N characters

Some scenarios

- Bundled 2LD variants
- TLD variants
- Parallel TLDs
- Individual trees

Bundled 2LD variants

- TLDs that bundle lexicographic variants
- Chinese: traditional and simplified
- Roman: accented and unaccented
- Greek: final ς in Νίκος.gr / ΝΙΚΟΣ.gr / Νικος.gr
- Usually implemented with common DNS
  - .gr uses DNAMEs, .cat did but switched

TLD variants

- Lexical variants of TLDs
- Example: .台湾 and .台灣
  - Currently implemented with DNAME

```
xn—kprw13d. IN DNAME xn--kpry57d.
```

Parallel TLDs

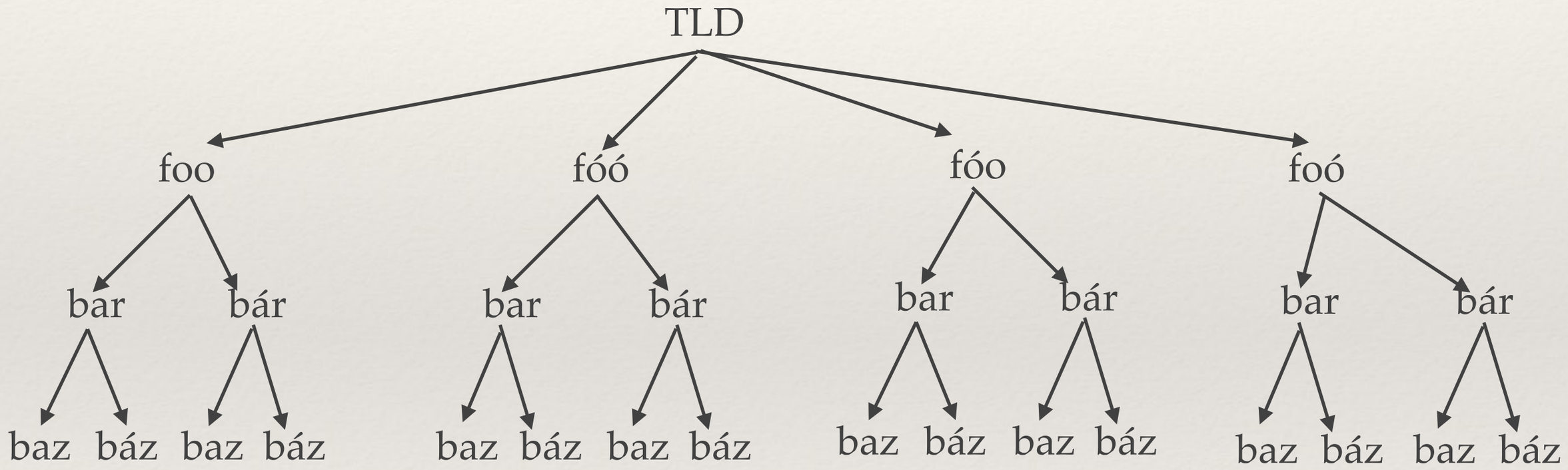
- TLDs that may be equivalent
- .中国 and .中國 have same NS, intended to have same contents
- .NGO and .ONG have same NS, not required to have same contents

Individual trees

- Separately registered names for the same entity
  - bigcorp.com / bigcorp.net
  - bright-color.cc / bright-colour.cc
- Up to the registrant to make it work

Subtrees

- Bundled names can occur at any level
- Exponential explosion



DNS and Applications

- Even if DNS is set up right, applications often fail
- Same DNS for fóó.biz and foo.biz, but Web server for `http://fóó.biz` doesn't handle `http://foo.biz`
- Similar problems for e-mail, anything that uses SRV
- Can applications configure themselves automatically?

Current approaches

- Parallel NS
- CNAME
- DNAME

Approach: parallel DNS

- Same name servers for all names in bundle
- Depends on DNS manager to keep zones in sync
- In practice, they don't

Approach: CNAMEs

- Parallel NS but one zone has CNAMEs at every name
- Operationally awful, no better than parallel DNS
- Doesn’t work with SMTP MX
- Delegated subtrees a problem
- Zone has no control over who points CNAMEs at it

Approach: DNAMEs

- Doesn't handle the name at the DNAME
  - OK for TLDs 台湾 and .台灣
    - Fatal flaw for 2LDs, didn't work in .cat
- Same SMTP MX problems
- Delegated subtrees don't work
- Zone has no control over who points DNAMEs at it

Proposed solutions

- BNAME
- CLONE
- Arc-pointers

Proposal: BNAME

- New RRTYPE BNAME
- Effect similar to CNAME+DNAME
- See draft-yao-dnsext-bname-06

Proposal: CLONE

- New RRTYPE: CLONE *name1 name2* …
- Authoritative server synthesizes *name1,* … records parallel to current zone
- Clone-aware cache can synthesize too
- See draft-barton-clone-dns-labels-fun-profit
- Avoids B/C/DNAME control problem

Proposal: Arc-pointers

- Slightly different question: can a single Internet name space have multiple resolution systems? (Think .onion)
- Pointer system within the DNS references alternate resolution systems that handle a part of the namespace.
- Bundled names have one set in the DNS, others in alternate system. Transform before re-consulting DNS is alternate resolution, e.g., .color.example -> .colour.example
- See `draft-hardie-arc-pointers`, notes risks & downsides.

Application issues

- When Web and mail servers see mystery domain names
  - Do DNS lookup to see if it's a BNAME/CLONE/…
  - Treat mystery name as known bundled name
- Is this a good idea?
  - Security issues from CNAME/DNAME/BNAME
  - TLS certificate names?

Next steps?